TELECOMMUNICATIONS DIVISION

AGENCY TELECOMMUNICATIONS REPRESENTATIVE

BULLETIN 02-11

AUGUST 7, 2002

SUBJECT: PREVENTION OF VOICE MAIL FRAUD

ACTION:

- Distribute copies of this bulletin to all Agency Telecommunications Representatives (ATRs), Accounts Payable staff, and voice mail users in your agency or department.

- Develop internal procedures based on this ATR and other reliable sources, to advise all employees with voice mail to be aware of the potential for fraudulent use of voice mail systems and how to take precautions to prevent fraud. These procedures should also encourage immediate reporting of suspicious calls or activity on voice mail accounts, and direct employees on how they should report this suspected fraud.

- Regularly review telephone bills, including the State Integrated Billing System (SIBS) invoices. Immediately contact your voice mail provider, or your SIBS billing account representative at 1-800-505-5400 if it appears that fraud has occurred, so that the investigation process can be quickly implemented.

KEY POINTS:

Each employee who uses voice mail must make it as difficult as possible for others to fraudulently use voice mail, and understand why their role is critical to maintaining voice mail security. This helps reduce charges attributable to fraudulent long distance calls.

- Individual voice mail users must:

    1. Ensure that their voice mail password is not easy to guess. For example, **do not use** the seven digit telephone number of the voice mailbox (default password); repeated or sequential numbers (e.g. 1111, 9999, 1234); or, the last four digits of the telephone number for a password.

    2. Check their voice mail greeting/message on a regular and frequent basis to make sure that it has not been changed without their knowledge. If a user is unable to access the voice mailbox or to change their password because the mailbox may have been co-opted, they should immediately follow internal procedures for notifying the voice mail provider. For California Integrated Information Network (CALNET) voicemail users, this is the California Major Accounts Center (CMAC) at 1-800-303-0103. Explain that it is an emergency due to fraud.

- In addition to the precautions above, customers with a Private Branch Exchange (PBX) or key system must:

    1. Review existing security procedures and develop internal processes to help ensure appropriate measures are taken to prevent fraud or inappropriate use of voice mail.

Proper programming of the PBX/key system is especially important to protect against fraud as noted in 2-4 below.

2. Disable or restrict the Direct Inward System Access (DISA) feature. DISA is the major method used by hackers to dial into a system to obtain long distance access.

3. Disable or restrict the international outbound calling capability.

4. Disable or restrict the ability to accept inbound collect calls.

- SBC/Pacific Bell has taken many steps to protect their CALNET voice mail systems from fraud, and will continue to monitor and upgrade as needed to prevent fraud.

BENEFITS:

- Will help minimize the opportunity to charge fraudulent calls to state and local government through preventive measures.

- Reporting potential fraud quickly will enable more effective fraud investigation and prevention, and help result in cost savings to state and local government.

BACKGROUND

A number of cases of voice mail fraud have recently been reported by users of CALNET. Voice mail systems have been hacked in various areas of the State, and fraudulent calls are being billed. Like the lock on your front door, voice mailboxes can be opened if someone has the key or password.

Hackers have developed sophisticated methods for identifying, opening and co-opting voice mailboxes to obtain long distance services without charge, and it can be very difficult to trace this use back to the originators. In the meantime, legitimate voice mailbox users are saddled with the costs incurred, which can quickly run into thousands of dollars. Prevention is the key.

To view other ATR bulletins, refer to the DGS Telecommunications Division website at http://www.td.dgs.ca.gov (click on Network Publications on the right side of the page, then scroll down to the ATR bulletins.)

If you have questions regarding this bulletin, please call the Resource Communication Center at (916) 657-9903, and request to speak to a Customer Account Manager.

BARRY R. HEMPHILL
Deputy Director for Telecommunications Division

BRH:SB:eas:pc